

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ГИБКИХ МЕТОДОЛОГИЙ РАЗРАБОТКИ АСУТП

*Е. В. Игорихина, научный руководитель: О. В. Михайлова
(г. Новокузнецк, Новокузнецкий институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования
«Кемеровский государственный университет»)
e-mail: 13sadzi@gmail.com, mi_o@ngs.ru*

A COMPARATIVE ANALYSIS OF AGILE METHODOLOGIES DEVELOPMENT OF PROCESS CONTROL SYSTEM

*E. V. Igorichina, O. V. Mikhaylova
(Novokuznetsk, Novokuznetsk Institute (branch) Federal state budgetary educational institution
of higher professional education "Kemerovo state University")*

Abstract. The paper presents a comparative analysis of agile development methodologies APCS. You can find descriptions of modern methodologies, principles and techniques.

Keywords: AGILE METHODOLOGIES, AUTOMATED CONTROL SYSTEM OF TECHNOLOGICAL PROCESSES, EXTREME PROGRAMMING, LEAN DEVELOPMENT METHODOLOGY, TEST-DRIVEN DEVELOPMENT

Повысить качество систем управления технологическими процессами (АСУТП) и сократить сроки их разработки может оптимальная организация труда.

С учетом текущего состояния научно-технического прогресса, требованиями сокращения сроков разработки и повышение качества систем (по критериям стандартов и требованиям заказчика) наиболее эффективными методологиями являются гибкие методологии разработки, такие как экстремальное программирование (XP), бережливая методология разработки (*Lean*), *SCRUM*, *KANBAN* и другие [1].

Их основные черты: изменение требований к продукту в процессе разработки, в первую очередь реализуются основные и необходимые функции; итерационный выпуск версий продукта, каждая из них тщательно тестируется; имеется постоянная обратная связь с заказчиком и основным потребителем продукта.

Основные методологии и их основные принципы представлены ниже.

1. Экстремальное программирование (XP) — гибкая методология разработки, авторами которой являются Кент Бек, Уорд Каннингем, Мартин Файлер и др. [2, 3]. Своё название методология получила из идеи применения полезных традиционных методов и практик разработки, подняв их на новый «экстремальный» уровень.

В данной методологии реализованы 12 основных приёмов (по первому изданию книги *Extreme programming explained*):

- Разработка через тестирование (*Test-driven development*)
- Игра в планирование (*Planning game*)
- Заказчик всегда рядом (*Whole team, Onsite customer*)
- Парное программирование (*Pair programming*)
- Непрерывная интеграция (*Continuous integration*)
- Рефакторинг (*Design improvement, Refactoring*)
- Частые небольшие релизы (*Small releases*)
- Простота (*Simple design*)
- Метафора системы
- Коллективное владение кодом (*Collective code ownership*)
- Стандарт кодирования (*Coding standard or Coding conventions*)
- 40-часовая рабочая неделя (*Sustainable pace, Forty-hour week*)

2. *Lean* — методология разработки, основанная на постоянном стремлении к устранению потерь [4]. Предполагает вовлечение в процесс разработки каждого сотрудника и максимальную ориентацию на потребителя. Впервые описана в книге Тома и Мэри Поппендик.

Данная методология реализует следующие принципы:

- Исключение потерь.
- Акцент на обучении.
- Предельно отсроченное принятие решений.
- Предельно быстрая доставка заказчику.
- Мотивация команды.
- Интегрирование.
- Целостное видение.

3. *Scrum* — методология, делающая акцент на качественном контроле процесса разработки [5]. Подход впервые описали Хиротака Такэути и Икудзиро Нонака. Они отметили, что проекты, над которыми работают небольшие команды из специалистов различного профиля, производят лучшие результаты.

В *Scrum* реализованы следующие принципы:

- Организация процесса разработки приложений в небольших командах.
- Выделение небольших требований и их распределение по важности.
- Короткие итерации
- Проведение собраний и обзоров.

4. *Kanban* — метод управления разработкой, реализующий принцип «точно в срок» и способствующий равномерному распределению нагрузки между работниками. Является наглядной системой разработки, которая демонстрирует, что необходимо производить, когда и сколько.

Канбан основан на четырёх основных принципах:

- Опора на существующие методы разработки.
- Предварительная договорённость о проведении важных изменений.
- Уважение к существующему порядку, ролям и обязанностям.
- Поощрение инициативы.

Все методологии, кроме Канбан, поддерживают короткие итерации (2-4 недели), они имеют различные области применения и особенности (например, для *XP* это постоянное корректирование проекта, для *Lean* — использование визуализирующих инструментов, для Канбан — упор на задачи, а для *Scrum* — высокий уровень коммуникации и взаимодействия внутри команды и четко прописанная формальная организация). Также во всех методологиях организуют небольшие команды разработчиков. Недостатком всех методологий, кроме *Scrum*, является риск формирования недисциплинированных команд, а недостатком *Scrum* является риск увеличения времени проекта.

Таким образом, каждая из методологий имеет ряд преимуществ, но наиболее интересным для создания АСУТП кажется экстремальное программирование. Положительными сторонами применения принципов экстремального программирования являются: сокращение времени процесса разработки АСУТП, сокращение процесса обучения сотрудников, распределение знаний и навыков между разработчиками, формирование корпоративных стандартов разработки и т. п.

ЛИТЕРАТУРА

1 Нестеров А. Л. Проектирование АСУ ТП [Текст] : Методическое пособие / А. Л. Нестеров. — СПб. : Издательство ДЕАН, 2006. — 522 с.

2 Бек К: Экстремальное программирование [Электронный ресурс]: электрон. текстовые дан. — Режим доступа: http://www.e-reading.club/bookreader.php/69190/Bek_-_Ekstremal'noe_programmirovanie.html

3 Экстремальное программирование — реальность и мифы [Электронный ресурс]: элек- трон. текстовые дан – Режим доступа: <http://skipy.ru/philosophy/xp.html>

4 Поппендик М. Бережливое производство программного обеспечения: от идеи до прибыли [Текст] / М. Поппендик. — М. : «Вильямс», 2009. — 256 с.

5 Кон М. Scrum: гибкая разработка ПО [Текст] / М. Кон — М. : «Вильямс», 2007. — 576 с.

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ СЕРВИСОВ АУТЕНТИФИКАЦИИ ПУТЕМ ПРОВЕДЕНИЯ ДОПОЛНИТЕЛЬНОЙ ИДЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ ОПТИМАЛЬНОГО ПРИЗНАКОВОГО ПРОСТРАНСТВА

А.Ю. Исхаков, С.Ю. Исхаков, Р.В. Мещеряков

*Томск (Томский государственный университет систем управления и радиоэлектроники)
iskhakovandrey@gmail.com*

INCREASE IN SECURITY OF AUTHENTICATION SERVICES THROUGH ADDITIONAL IDENTIFICATION USING OPTIMAL FEATURE SPACE

A.Y. Iskhakov, S.Y. Iskhakov, R.V. Meshcheryakov

Tomsk (Tomsk State University of Control Systems and Radioelectronics)

Abstract. The research focuses on topical issue of the Internet security. In particular, the issue of level increase in security of authentication services through additional identification using optimal feature space is being considered. This article is devoted to the practical application of additional identification technologies in authentication services. The paper presents sets of informative features characterizing the access subject. A classification of methods for identifying the user's work environment is proposed. The article presents the experimental results of intercomparison between scientifically-grounded methods and technologies for identifying the user's work environment.

Keywords: authentication; identification; information security; IoT; identification methods; attribute; user; browser fingerprint; cookies.

Введение. Сегодня глобальная сеть Интернет день является одним из основных инструментов массовых коммуникаций. Ее стремительное развитие неразрывно связано с новыми научными открытиями и технологическими инновациями в различных сферах it-индустрии. Данные обстоятельства способствуют развитию информационных систем самого разного профиля, обеспечивающих возможность удаленного взаимодействия с пользователями. С увеличением объема пользовательских данных в сети неразрывно растет и количество различных киберугроз [1].

Эта проблема в частности характерна для инфраструктуры Интернета вещей (IoT) [2, 3]. Одной из важных задач в обеспечении защиты элементов сетевых систем, в том числе таких как IoT, является реализация эффективного функционала по контролю и управлению доступом для пользователей, осуществляющих удаленные подключения к элементам сети, а также smart-устройствам [4]. В частности, в рамках данного исследования будут рассмотрены вопросы повышения защищенности сервисов аутентификации путем проведения дополнительной идентификации субъектов доступа.

Необходимость проведения дополнительной идентификации. Рассмотрим перспективную инфраструктуру облачного видеонаблюдения в концепции IoT. Подобные комплексы давно перестали быть просто системами, транслирующими видео с камеры на устройство для просмотра. Сегодня настала эпоха облачного видеонаблюдения: удаленного smart-мониторинга, не нуждающегося в постоянном контроле оператора. Активное видеонаблюдение способно анализировать видеопоток в режиме реального времени и уведомлять пользователя о возможных инцидентах.